

FORM PTO-1390
(Rev. 10-96)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

032326-093

SEP 20 2000

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.51)
Unassigned 09/646586INTERNATIONAL APPLICATION NO.
PCT/FR99/50292INTERNATIONAL FILING DATE
10 February 1999PRIORITY DATE CLAIMED
20 March 1998

TITLE OF INVENTION

METHOD FOR SECURELY MANAGING A UNITS COUNTER AND SECURITY MODULE IMPLEMENTING SAID METHOD

APPLICANT(S) FOR DO/EO/US

Carole-Audrey KOCH-HOURRIEZ, Mireille PAULIAC and Xavier BACHELIN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

U.S. APPLICATION NO. (If known, use 37 CFR 1.53) 09/646566 Unassigned		INTERNATIONAL APPLICATION NO PCT/FR99/00292		ATTORNEY'S DOCKET NUMBER 032326-093	
---	--	--	--	--	--

17. <input checked="" type="checkbox"/> The following fees are submitted:				CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO \$840.00 (970) International preliminary examination fee paid to USPTO (37 CFR 1.482) \$670.00 (956) No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) \$690.00 (958) Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$970.00 (960) International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$96.00 (962)					
ENTER APPROPRIATE BASIC FEE AMOUNT =					
Surcharge of \$130.00 (154) for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492(e)). 20 <input type="checkbox"/> 30 <input type="checkbox"/>				\$ -0-	
Claims	Number Filed	Number Extra	Rate		
Total Claims	13 - 20 =	-0-	X\$18.00 (966)	\$ -0-	
Independent Claims	2 - 3 =	-0-	X\$78.00 (964)	\$ -0-	
Multiple dependent claim(s) (if applicable)			+ \$260.00 (968)	\$ -0-	
TOTAL OF ABOVE CALCULATIONS =				\$ 840.00	
Reduction for 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				\$ -0-	
SUBTOTAL =				\$ 840.00	
Processing fee of \$130.00 (156) for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492(f)). 20 <input type="checkbox"/> 30 <input type="checkbox"/>				\$ -0-	
TOTAL NATIONAL FEE =				\$ 840.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 (581) per property +				\$ -0-	
TOTAL FEES ENCLOSED =				\$ 840.00	
				Amount to be: refunded	\$
				charged	\$

a. ☒ A check in the amount of \$ 840.00 to cover the above fees is enclosed.


b. ☐ Please charge my Deposit Account No. 02-4800 in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404


 SIGNATURE

 James A. LaBarre
 NAME

28,632
 REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
)
Carole-Audrey KOCH-HOURRIEZ et al) Group Art Unit: Unassigned
)
Application No.: Unassigned) Examiner: Unassigned
)
Filed: September 20, 2000)
)
For: METHOD FOR SECURELY)
MANAGING A UNITS COUNTER)
AND SECURITY MODULE)
IMPLEMENTING SAID METHOD)

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title, insert the following:

--This disclosure is based upon, and claims priority from French Patent Application No. 98/03483, filed March 20, 1998, and International Application No. PCT/FR99/00292, filed February 10, 1999, the contents of which are incorporated herein by reference.

Background of the Invention--.

Page 2, lines 13-14, delete “since is” and insert --due to the--;

lines 14-15, delete “is great the” and insert --the high--.

Page 4, before line 9, insert the following heading:

--**Summary of the Invention** --.

Page 9, before line 14, insert the heading:

--**Brief Description of the Drawing**--;

Page 10, before line 1, insert the heading:

--**Detailed Description**--;

Page 10, line 14, change “splitin” to --split in --.

IN THE CLAIMS:

1. (Amended) A method for the protected management of a unit counter in an electrically erasable and programmable memory, according to which the number of units consumed by users is recorded by means of a counter, [characterised in that it consists in breaking down] comprising the following steps:

dividing the unit counter into at least two memory areas; [(A, B), a first area (A) in which]

storing at least one bit [is stored] per at least one consumed unit into a first memory area; [and a second area (B) in which the]

storing a value corresponding to the total units consumed in a second
memory area; and [is stored],

updating the second area [being updated] only when the number of units
consumed exceeds or attains the number of bits not stored [bits of] in the first area [(A)].

2. (Amended) A method of managing a counter according to Claim 1,
[characterised in that] wherein the units consumed are recorded in the first area [(A)]
cyclically.

3. (Amended) A management method according to [Claims 1 and 2,
characterised in that] claim 1, wherein an operation of recording n units consumed
comprises the following steps:

- reading the content of the first area [(A)] and comparing the number of
not stored bits (L) in the first area [(A)] with the number of consumed units (n) to be
recorded,
- if [this] the number of not stored bits (L) is greater than or equal to the
number of units (n) to be recorded, storing the bits (n) to be recorded [are stored in the] in
said first area [(A)],
- if [this] the number (L) is less [,] than n, storing L bits [are stored] in the
first area [(A)] and [the] recording (n-L) remaining units [are recorded] in the second area
[(B)] by performing an operation of updating this area, and
erasing the first area [(A) is erased].

4. (Amended) A management method according to [any one of Claims 1 to 4, characterised in that] claim 3, wherein an operation of updating the second area [(B)] comprises a step of writing in this second area a new coded counter value equal to the current value to which the number of stored bits in the first area [(A)] and the (n-L) remaining consumed units to be stored are added.

5. (Amended) A management method according to Claim 4, [characterised in that] wherein the updating comprises a prior step of recording indicator information [(C2)] signifying that an updating is currently being carried out.

6. (Amended) A management method according to [any one of the preceding claims, characterised in that] claim 5, wherein the unit counter has an area [(SB)] for backing up the second area [(B)] and [in that] these two areas each have a field for recording a redundancy code [(CR, SCR)], for checking the integrity of the content of these two areas.

7. (Amended) A management method according to [Claims 4 and 5, characterised in that] claim 6, wherein an operation of recording n units consumed also comprises a prior step of verifying the state of the counter comprising the following operations:

- verifying the absence of the indicator information for a current update:
 - where the indicator information is [indeed] absent:

00260" 9954960

- [verification of] verifying the validity of the fields
containing the redundancy codes:

- . where the fields are valid:
 - recording [of] the n units;
- . where the fields are not valid:
 - detection of a fault and stoppage of the counter,
- where the indicator information is present:
 - activation of the recovery operation to re-establish the
integrity of the contents of the counter.

8. (Amended) A management method according to [Claims 6 and 7,
characterised in that] claim 7, wherein an operation of updating the second area [(B) then]
includes the following steps:

- recording the indicator information [(C2)],
- copying, in the backup area [(SB)], the coded value [(V0)] of the counter
of the second area [(B)],
- recording the new coded value of the counter in the second area [(B)],
- erasing the indicator information [(C2)].

9. (Amended) A management method according to Claim 8, [characterised in
that] wherein the recovery operation [consists in] comprises determining at which step the
abnormality occurred, and then performing, according to the circumstances determined, the

steps of updating at least one of the backup area, [(SB) and/or of] the second area [(B) and/or of] and the first area [(A)].

10. (Amended) A management method according to Claim 9, [characterised in that] wherein the determination of the step at which the abnormality occurred [consists in] comprises reading the content of each of the areas in order to determine whether the abnormality occurred during the updating of the backup area [(SB)], case 1, during the updating of the second area [(B)], case 2, during the erasure of the first area [(A)], case 3, between the updating of the second area [(B)] and the backup area [(SB)], case 4, or after the updating of these two areas, case 5, and:

[. in] for case 1 [in]:

- copying the value contained in the second area [(B)] into the backup area [(SB)],

- updating the second area [(B)] by recording the new value which is equal to the old one to which the content of the first area [(A)] is added,

- erasing the first area [(A)], and

- erasing the indicator information [(C2)];

[. in] for case 2 [in]:

- copying into the second area [(B)] the value contained in the backup area [(SB)] by adding the value contained in the first area [(A)],

- erasing the first area [(A)], and

- erasing the indicator information [(C2)];

[. in] for case 3 [in]:

- erasing the content of the first area [(A)], and
- erasing the indicator information [(C2)];

[. in] for case 4 [in]:

- implementing the steps according to case 2;

[. in] for case 5 [in]:

- implementing the steps according to case 3.

11. (Amended) A management method according to [any one of the preceding claims, characterised in that it comprises] claim 5, further including the step of recording information signifying a failure [(C1)] in reading or writing to the first area, [(A)] deactivating [the] said area when it has not been possible to read or write in this area, [and a step of reading this] reading said information signifying a failure at each new cycle, and directly recording the units consumed [then being directly recorded] in a coded manner by an operation of updating the second area [(B)].

12. (Amended) A management method according to [Claim 5 and] Claim 11, [characterised in that] wherein the information [(C2)] indicating a current updating and the information signifying a failure [(C1)] in reading and writing to the first area are recorded in a third area [(C)] of [the] said counter.

Cancel claims 13 and 14, and add the following new claims:

--15. A security module for the protected management of a unit counter in which the number of units of a commodity consumed by users is recorded, comprising:

a first memory area having a predetermined bit capacity, in which at least one bit is stored for each unit that is consumed;

a second memory area in which a value indicating the total number of consumed units is stored; and

a control mechanism which updates the value stored in said second memory area when the sum of the number of units consumed plus the number of bits stored in said first area is at least equal to the bit capacity of said first memory area.

16. The security module of claim 15, wherein said security module is contained in a terminal that manages the consumed units.

17. The security module of claim 16, wherein said terminal is a telephony terminal.--


000250 " 03537560

REMARKS

Entry of the foregoing amendments is respectfully requested. These amendments are intended to further clarify the language of the claims and specification, as well as eliminate multiple dependencies.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: September 20, 2000

000250" 99594950

4/PR45

000250 " 68524360

A METHOD FOR THE PROTECTED MANAGEMENT OF A UNIT COUNTER AND A SECURITY MODULE IMPLEMENTING THE METHOD

The object of the present invention is a method for the protected management of a unit counter located in memory, in particular a chip card in relationship with a terminal. It could nevertheless apply to any other type of memory.

The invention is particularly useful when it is a case of counting a very large number of units whilst preserving the storage capacity of the memory.

The storage capability of the memory (its suitability for being updated) is limited in time because of the technology used by the manufacturers of

electrically erasable and programmable non-volatile memories (for example EEPROMs).

The manufacturers guarantee the good behaviour of the memory for a limited number of updates of the memory (an update comprises an erasure operation followed by a programming or writing). Beyond that, the memory may no longer be correctly erased or correctly programmed.

On average, the number of updates guaranteed by the memory manufacturers is around 100,000 per memory location. In the case of a unit counter, the problem consisting in preserving the storage capability of the said counter is all the more difficult to resolve since is high the number of units to be counted and is great the frequency of updating of the counter.

The invention will be described in particular in the case of an application to a chip card in the field of cardphones.

It is known, in the field of chip cards, that a transaction between a terminal and an external electronic purse is organised around a security module (SM) comprising a microprocessor. The module is generally integrated into the terminal.

The role of a security module is particularly to ensure the verification of the authentication of the electronic purse cards external to the terminal. In the context of cardphones, the electronic purse chip card is a phone card (not reloadable), the terminal is a cardphone (or telephone box) and the security module

000250" 9954350

It should be noted that the set of commands of the component of the said security module is referred to as the "operating system".

In addition to the authentication functions, the module proposes to the operator of a cardphone to manage, in a secure manner, a unit counter which records all the units consumed by the different holders of prepayment cards or phone cards during telephone communications made from the said cardphone.

Still in the context of cardphones, such a counter must be able to store 16 million units, which corresponds to a maximum number of telephone units able to be recorded at very highly frequented public places (such as airports) for measurements made over the average lifetime of the counters of a cardphone (approximately 3 years).

The updating of the said counter can also be required on several occasions during a telephone communication.

In order to store as many units using the counters of the prior art it would be necessary to use a 24-bit memory. However, in this case, the number of updates would exceed the storage capacity of this memory. This solution can therefore not be envisaged.

In the invention, provision has been made for remedying this problem by breaking down the unit counter into at least two main areas.

The first memory area of the counter (zone A) is considered to be a bit field. A consumed communication unit corresponds to each bit stored or "blown" or "written" or "switched on". A "token" is also spoken of to characterise a bit stored in area A.

A second, smaller, memory area (area B), whose size makes it possible to code the maximum value of the number of units to be stored.

These memory areas are memory areas of an electrically programmable and electrically erasable non-volatile memory.

With regard to area A and without going into the technology of the programming of memories, a memory location will be considered to be unavailable when a bit is stored therein. Hereinafter the term stored bit or "switched-on bit" or "blown bit" or written bit will be used indifferently to mean that the memory locations are unavailable, and switched-off or not blown bit to mean that the locations are available (free).

A switched-on bit will be made available (switched off) only at the next erasure of the entire area A (switching off of all the bits making it up).

The units consumed are recorded in the first area cyclically.

An operation of recording n units consumed comprises the following steps:

- reading the content of the first area and comparing the number of not stored bits with the number of consumed units to be recorded,

- if this number of not stored bits is greater than or equal to the number of units to be recorded, the bits to be recorded are stored in the said area,

- if this number is less, this number of bits is stored in the first area and the remaining units are recorded in the second area by performing an operation of updating this area, and the first area is erased.

An operation of updating the second area (B) comprises a step of writing in this second area a new coded counter value equal to the current value to which the number of not blown bits in the first area (A) and the remaining consumed units to be stored are added.

The updating of the second area comprises a prior step of recording indicator information meaning that an updating is taking place, then, when the updating is ended, the updating consists in erasing the first area (A) and erasing the indicator information.

To improve security the unit counter has an area (SB) for backing up the second area (B) and these two areas each have a field for recording a redundancy code (CR, SCR), for checking the integrity of the content of these two areas.

An operation of recording n units consumed also comprises a prior step of verifying the state of the counter comprising the following operations:

- verifying the absence of the indicator information for a current update:

- where the indicator information is indeed absent:

000260"8354350

. where the fields are valid:

. where the fields are not valid:

- where the indicator information is present:

An operation of updating the second area then describes the following steps:

- recording the indicator information,

- recording the new coded value of the counter in

- erasing the indicator information.

The recovery operation consists in determining at

Advantageously, the determination of the step at

the second area (B), case 2, during the erasure of the first area (A), case 3, between the updating of the second area (B) and the backup area (SB), case 4, or after the updating of these two areas, case 5.

In practical terms, the recovery consists in case 1 in :

- copying the value contained in the second area (B) into the backup area (SB),

- updating the second area (B) by recording the new value which is equal to the former one to which the content of the first area (A) is added,

- erasing the first area (A),

- erasing the indicator information (C2);

in case 2 in :

- copying into the second area (B) the value contained in the backup area (SB), adding the value contained in the first area (A),

- erasing the first area (A),

- erasing the indicator information (C2);

in case 3 in :

- erasing the content of the first area (A),

- erasing the indicator information (C2);

in case 4 in :

- implementing the steps according to case 2;

in case 5 in :

- implementing the steps according to case 3.

Advantageously the method also comprises a step of recording information signifying a failure in reading or writing to the first area (A) deactivating the said area when it has not been possible to read or write in

000250" 02594350

this area, and a step of reading this information at each new cycle, the units consumed then being directly recorded in a coded manner by an operation of updating the second area (B).

The information (C2) indicating a current updating and the information signifying a failure (C1) in reading and writing to the first area are recorded in a third area (C) of the said counter.

The invention also relates to a security module implementing the method according to the invention.

Such a module can be located in a terminal managing units consumed by the users of the terminal, and can also be in particular a telephony terminal.

Other particularities and advantages of the invention will emerge from a reading of the description below, which is given by way of non-limitative example with regard to the accompanying drawings, in which:

- Figure 1 schematically depicts the unit counter according to the invention;
- Figure 2A depicts the steps of recording n units according to the method of the invention;
- Figure 2B depicts the prior verification step 10 of Figure 2A;
- Figure 3 depicts the steps of recording the units in the second area (updating) according to a preferred embodiment;
- Figure 4 depicts the steps of the recovery mechanism;
- Figure 5 illustrates a variant in the according to the invention.

000250 " 69564360

In the example application given below, and which corresponds to the case of cardphones referred to in the introduction, the units consumed are telephone units and the sizes of areas A and B are obviously defined here for the purpose of example.

Area B is in turn split in order to overcome problems of cutting off of current during the updating of the counter (cf Figure 1). This case is detailed below.

As already mentioned, the operating life of the counter is directly related to the number of updates (erasure and writing). It is therefore essential to find a counter structure and a counting method which reduces the number of updates.

In the context of the invention, the storage of the communication units consumed takes place as follows.

It is assumed that the duration of a telephone communication is divided into time intervals. The duration of a time interval corresponds to a fixed number of consumed units. In this example, the

recording cycle for the consumed units is defined by these time interval.

At the start of each time range, the number of units consumed must be stored in the security module.

Thus, in the case of a communication requiring 13 units in total and where an elementary time interval comprises 3 units, the unit counter within the security module will be updated five times during the communication and a sixth time at the end of the communication time.

The method of managing the unit counter is defined by steps 10, 20, 30, 40, 50 and 60 illustrated by Figure 2A.

A step prior to the recording of the units consists in checking the state of the counter (step 10) detailed from Figure 2B.

At each request to store consumed units, the operating system of the security module managing the counter checks that the number of switched-off (available) bits in the area A is greater than or equal to the number of units to be stored (cf Figure 2A).

In the affirmative, if n units have been consumed, n bits available in the area A are blown (provision can be made, by way of a variant according to the invention, for n bits available in the area A to be blown for n packets of consumed units).

This operation requires no erasure and only one action of writing amounts to blowing certain bits in the area A.

memory locations making up the area A and consequently area B.

The frequency of erasing and writing to the memory locations making up the unit counter is directly related on the one hand to the size of the area A and on the other hand to the granularity used for breaking down a communication (granularity means an elementary communication period corresponding to a number of units predetermined by the operator).

It should be noted that, in order to know at any time the total number of units consumed by means of the cardphone, it suffices to add, to the current value of the area B, the number of blown bits in the area A.

In the context of the invention, it is proposed to use an additional functionality for extending the service life of the unit counter.

This is because it is known that a bit field is subdivided into sets of consecutive eight bits known as bytes. As is described above, the area A is erased as frequently as the area B. However, for programming facilities or constraints related to the component used, blowing a bit within a byte may give rise to a new blowing of bits already blown within the said byte.

Thus a byte belonging to the area A can be written to more often (that is to say its bits blown) than a byte making up the area B. The area A then being more stressed than the area B, the operating life of the counter is therefore directly related to the storage capacity of the area A.

0000250 " 0000000000

To overcome this problem, it is proposed, in the context of the invention, to provide, within the unit counter, an additional memory area known as area C comprising at least one location for storing the information C1 (cf Figure 1 and Figure 5).

This variant of the method is illustrated by Figure 5.

In this variant, the step of verifying the state of the counter, prior to the recording of the consumed units, includes a reading of the area C in order to check whether the information C1 exists.

This information C1 is written as soon as a memory location in the area A can no longer be erased or written to (since provision is made in a conventional manner to check the correct execution of a writing or erasure in the memory). In this case the operating system of the security module decides to deactivate the area A (step 42) and to work only with the area B (step 80). With each request to store consumed units the area B is erased and rewritten.

Quite obviously, the storage capacity of the area B will in turn be rapidly impaired but the counter can continue to be used for some time more.

Moreover, in order to increase the security of the management of the counter, it is possible to add a mechanism for guaranteeing a coherent state of the said counter, if a cutting off of current occurs during the storage operation. It is not pertinent to envisage an operation of pulling out the security module since generally this is fully integrated into the cardphone.

Having said this, the case of pulling out would be managed in the same way.

In the context of the invention, in order to install such a mechanism (hereinafter referred to as a recovery mechanism), the area B is provided with a redundancy code. In addition the area B is duplicated (cf Figures 1, 2B and 3).

The area SB thus defined is used as a backup for the previous one. It is updated before any change to the area B.

The area SB contains at any time the value of the area B, preceding the last updating of the said area.

An additional byte within the area C is used to indicate whether the storage operation has been partially or entirely performed; this is the indicator information C2.

Thus, at the start of processing of a request to store units, C2 is stored. It is erased once this same storage operation has been fully carried out. To avoid excessively stressing the byte C2, the latter is used (written and then erased) only in the case where the number of units to be stored is greater than the number of bits still available in the area A.

If this is not the case, the byte C2 is unused. Amongst the available bits in the area A, n bits are switched on. The storage operation is terminated. It is considered that the loss of information is minimal.

Where the number of bits available within the area A is insufficient, it is essential to activate the

000260" 99594360

This is because, if a cutting off of current occurs after the area B has been erased and not once again rewritten to, all the information in the unit counter would be lost.

The system checks the absence of the indicator C2
(11).

If these fields are valid (13), the n units consumed are recorded.

In the case where the indicator exists (15), there is a use of the recovery mechanism detailed from the figure.

As can be seen in Figure 3 (steps 51 to 55), the indicator C2 is first of all written, and the current value, for example V0, of the counter coded in the area B is copied into the area SB. Then the area B is updated (new value V1 equal to the current value to which the number of bits blown in the area A and the n-L units remain to be stored are added). The area A is next erased and the indicator C2 is then erased to

indicate that the storage operation has been performed entirely with success.

In the description given, everything occurs normally, there has not been any cutting off of power during the storage operation.

Now, if a cutting off has occurred, the activation of the recovery mechanism is described below (cf Figure 4).

This is activated at the time of the next request to store whether or not the number of bits available within the area A is sufficient to store the n units.

If the indicator C2 is switched on, then, before storing the consumed units, the recovery mechanism is actuated by the operating system of the security module.

Several cases may occur. This is because the cutting off may have occurred during the updating of the area SB (case 1), during the updating of the area B (case 2), during the erasure of the area A (case 3) or between the said updatings (case 4 and case 5).

The recovery procedure must be distinct according to the different cases listed above.

Where the area SB has not been able to be correctly updated (case 1), the redundancy code SCR thereof is not in conformity. The value V0 contained in the area B is then copied into the area SB, the area B is then updated (new value V1 equal to the current value V0 of the area B to which it is necessary to add the number of blown bits in the area A, value VA).

Only the number of units $n-L$ which were to be stored during the interrupted storage is lost.

The area A is then erased and the indicator C2 too.

In the case where the area SB has been correctly updated but the area B has not been correctly updated (case 2), the redundancy code SCR of the area SB is correct. On the other hand, the redundancy code CR of the area B is incorrect.

The area B is then updated as follows:

The new value $V1$ of the area B is equal to the value $V0$ of the area SB, to which the number of blown bits in the area A, that is to say a value VA , $V1 = V0 + VA$, is added.

In this case as in the previous one, the only information lost corresponds to the number $n-L$ of units remaining which were to be stored during the interrupted storage. The area A is then erased and the indicator C2 too.

By examining only the redundancy codes of the area SB and of the area B, it is impossible to know whether the cutting off of current took place between the updating of the areas SB and B (case 4) or after the updating of these two areas (case 5). This is because in both cases the redundancy codes are both correct.

To distinguish cases 4 and 5, the operating system of the security module compares the values of the areas SB and B; $V(SB) = V(B)?$:

If the area SB contains the same value as the area B then the cutting off of the power must have taken

000250" 29534360

CLAIMS

1. A method for the protected management of a unit counter in an electrically erasable and programmable memory, according to which the number of units consumed by users is recorded by means of a counter, characterised in that it consists in breaking down the unit counter into at least two memory areas (A, B), a first area (A) in which at least one bit is stored per at least one consumed unit and a second area (B) in which the value corresponding to the total units consumed is stored, the second area being updated only when the number of units consumed exceeds or attains the number of not stored bits of the first area (A).

2. A method of managing a counter according to Claim 1, characterised in that the units consumed are recorded in the first area(A) cyclically.

3. A management method according to Claims 1 and 2, characterised in that an operation of recording n units consumed comprises the following steps:

- reading the content of the first area (A) and comparing the number of not stored bits (L) in the first area (A) with the number of consumed units (n) to be recorded,

- if this number of not stored bits (L) is greater than or equal to the number of units (n) to be recorded, the bits (n) to be recorded are stored in the said first area (A),

- if this number (L) is less, L bits are stored in the first area (A) and the (n-L) remaining units are recorded in the second area (B) by performing an

. where the fields are valid:

- recording of the n units;

. where the fields are not valid:

- detection of a fault and stoppage of the counter,

- where the indicator information is present:

- activation of the recovery operation to re-establish the integrity of the contents of the counter.

8. A management method according to Claims 6 and 7, characterised in that an operation of updating the second area (B) then includes the following steps:

- recording the indicator information (C2),
- copying, in the backup area (SB), the coded value (V0) of the counter of the second area (B),
- recording the new coded value of the counter in the second area (B),
- erasing the indicator information (C2).

9. A management method according to Claim 8, characterised in that the recovery operation consists in determining at which step the abnormality occurred, and then performing, according to the circumstances determined, the steps of updating the backup area (SB) and/or of the second area (B) and/or of the first area (A).

10. A management method according to Claim 9, characterised in that the determination of the step at which the abnormality occurred consists in reading the content of each of the areas in order to determine whether the abnormality occurred during the updating of the backup area (SB), case 1, during the updating of

000250 " 032000

the second area (B), case 2, during the erasure of the first area (A), case 3, between the updating of the second area (B) and the backup area (SB), case 4, or after the updating of these two areas, case 5,

. in case 1 in:

- copying the value contained in the second area (B) into the backup area (SB),

- updating the second area (B) by recording the new value which is equal to the old one to which the content of the first area (A) is added,

- erasing the first area (A),

- erasing the indicator information (C2);

. in case 2 in:

- copying into the second area (B) the value contained in the backup area (SB) by adding the value contained in the first area (A),

- erasing the first area (A),

- erasing the indicator information (C2);

. in case 3 in:

- erasing the content of the first area (A),

- erasing the indicator information (C2);

. in case 4 in:

- implementing the steps according to case 2;

. in case 5 in:

- implementing the steps according to case 3.

11. A management method according to any one of the preceding claims, characterised in that it comprises the step of recording information signifying a failure (C1) in reading or writing to the first area (A) deactivating the said area when it has not been

possible to read or write in this area, and a step of reading this information at each new cycle, the units consumed then being directly recorded in a coded manner by an operation of updating the second area (B).

12. A management method according to Claim 5 and Claim 11, characterised in that the information (C2) indicating a current updating and the information signifying a failure (C1) in reading and writing to the first area are recorded in a third area (C) of the said counter.

13. A security module (SM) implementing the method according to any one of the preceding claims.

14. A security module according to Claim 13, characterised in that it is installed in a terminal managing the consumed units, notably a telephony terminal.

000250" 000250" 000250"

ABSTRACT

The invention relates to a method for the protected management of a unit counter in an electrically erasable and programmable memory, according to which the number of units consumed by users is recorded by means of a counter, consisting in breaking down the unit counter into at least two memory areas (A, B), a first area (A) in which one bit is blown per unit consumed and a second area (B) in which the value corresponding to the total units consumed is stored, the second area being updated only when the number of units consumed exceeds or attains the number of not blown bits in the first area.

Application to the security modules placed in telephone terminals.

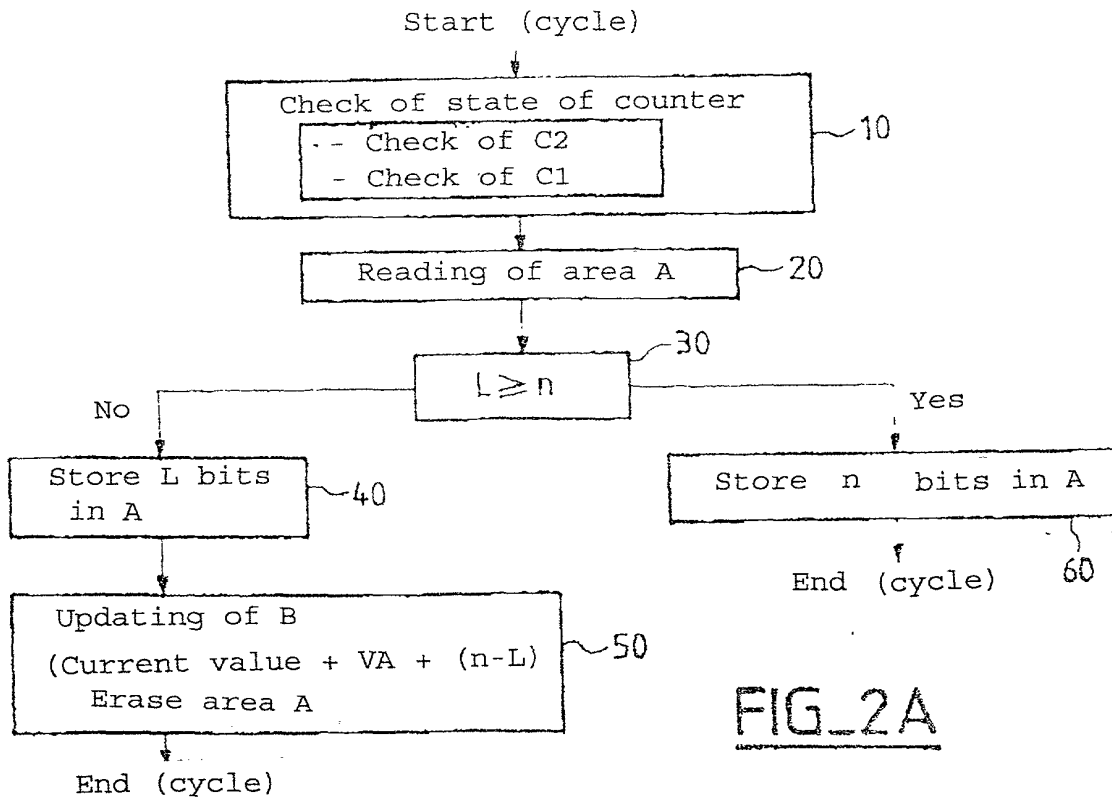
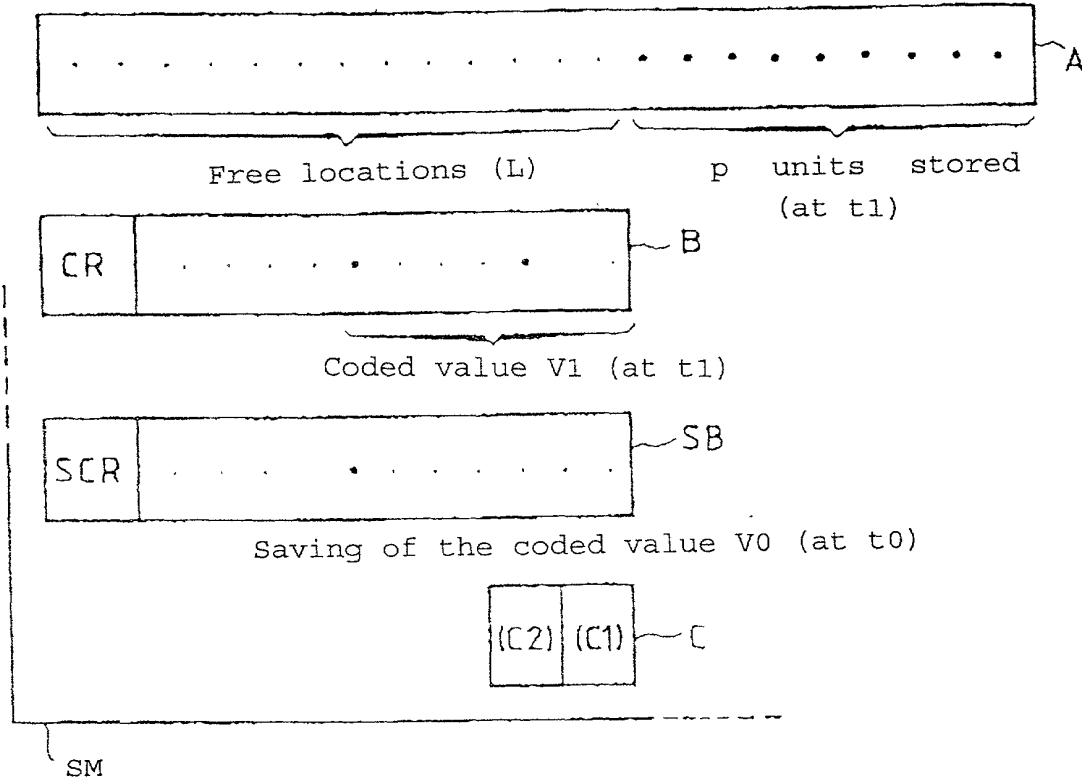
Figure 2A

000260" 99544567

WO 99/49646

PCT/FR99/00292

1/4
FIG_1



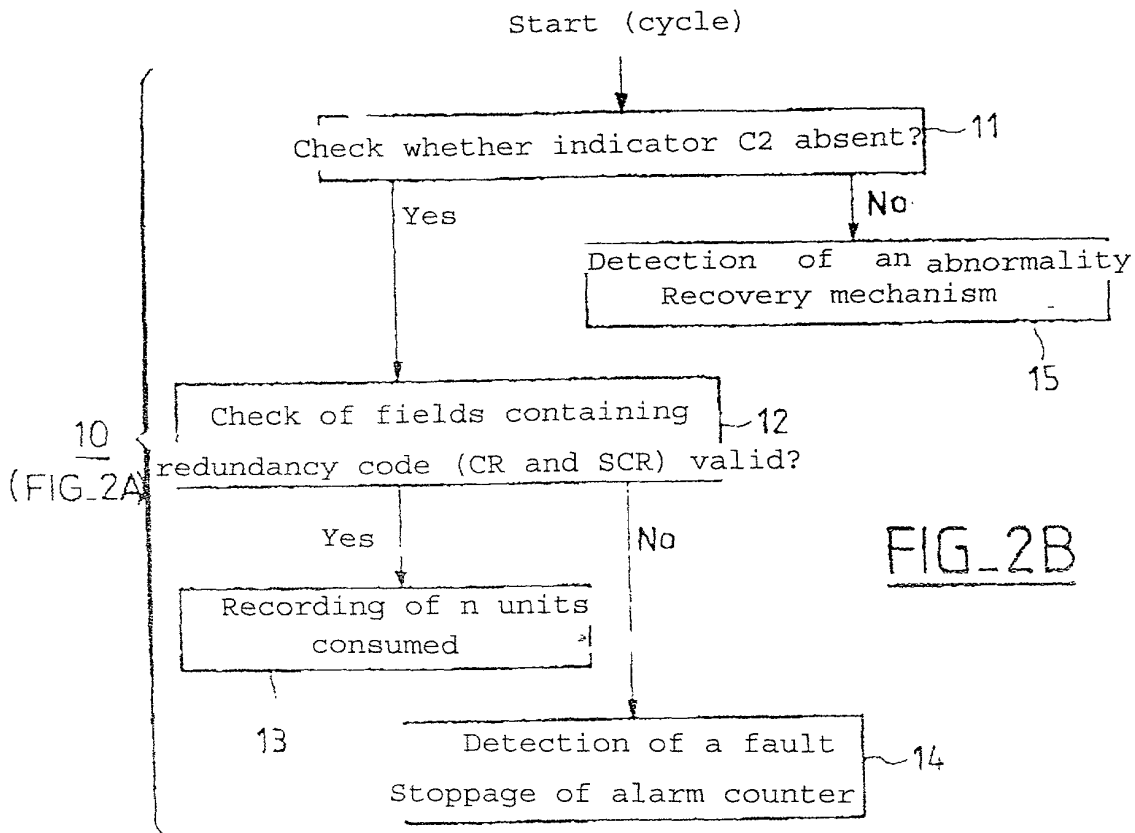
FIG_2A

000260 9959466

WO 99/49646

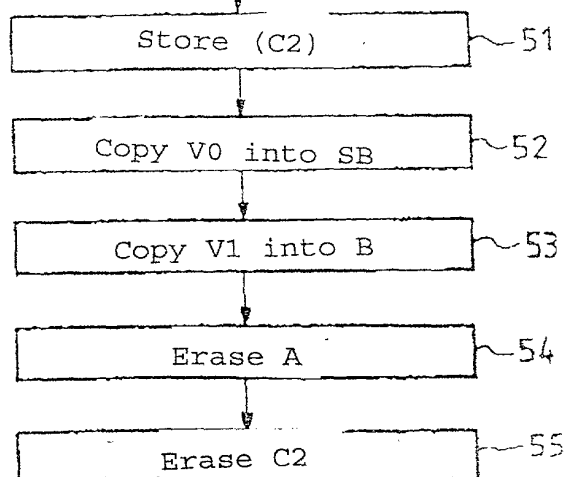
PCT/FR99/00292

2/4



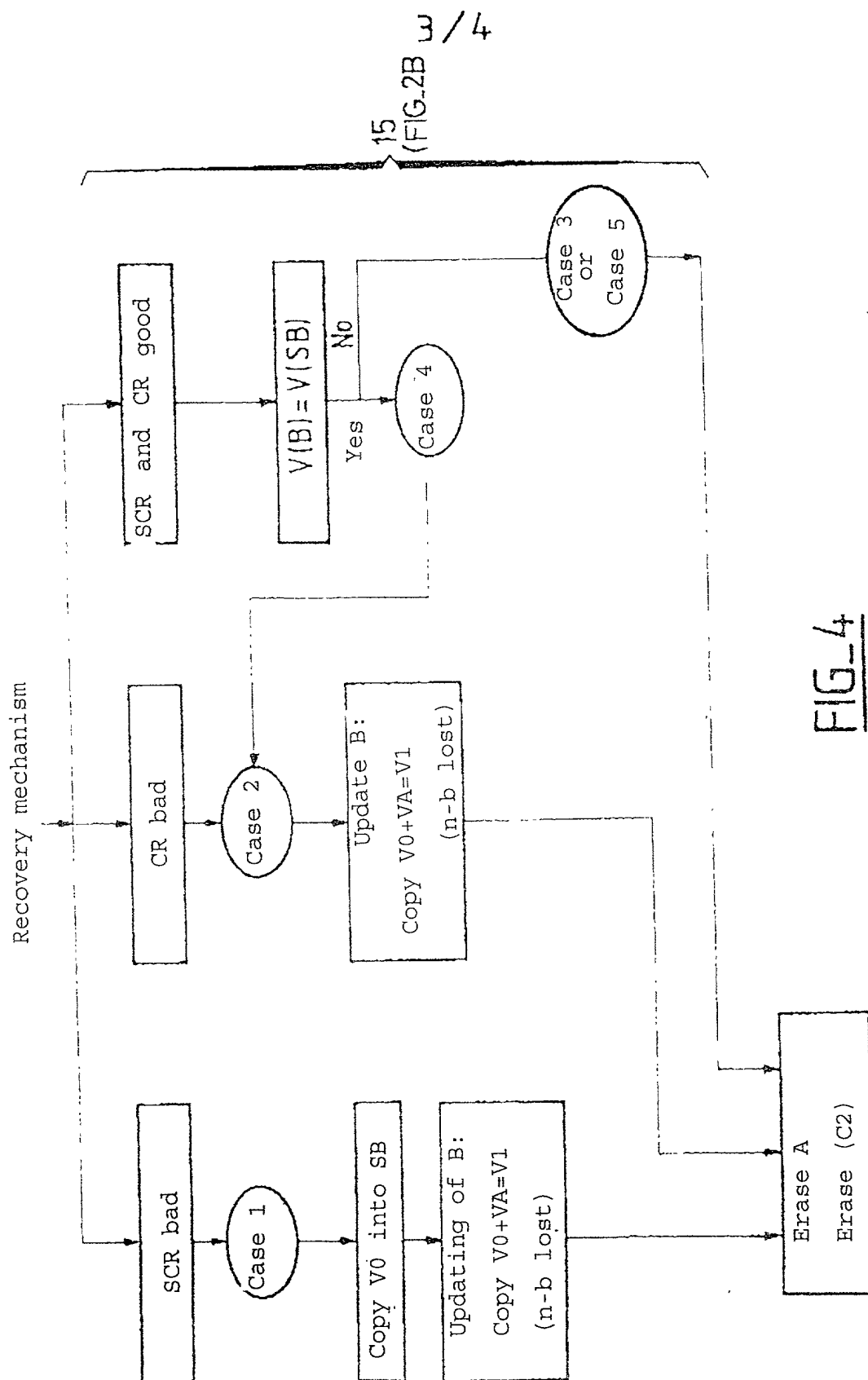
FIG_3

Updating of B (50)



WO 99/49646

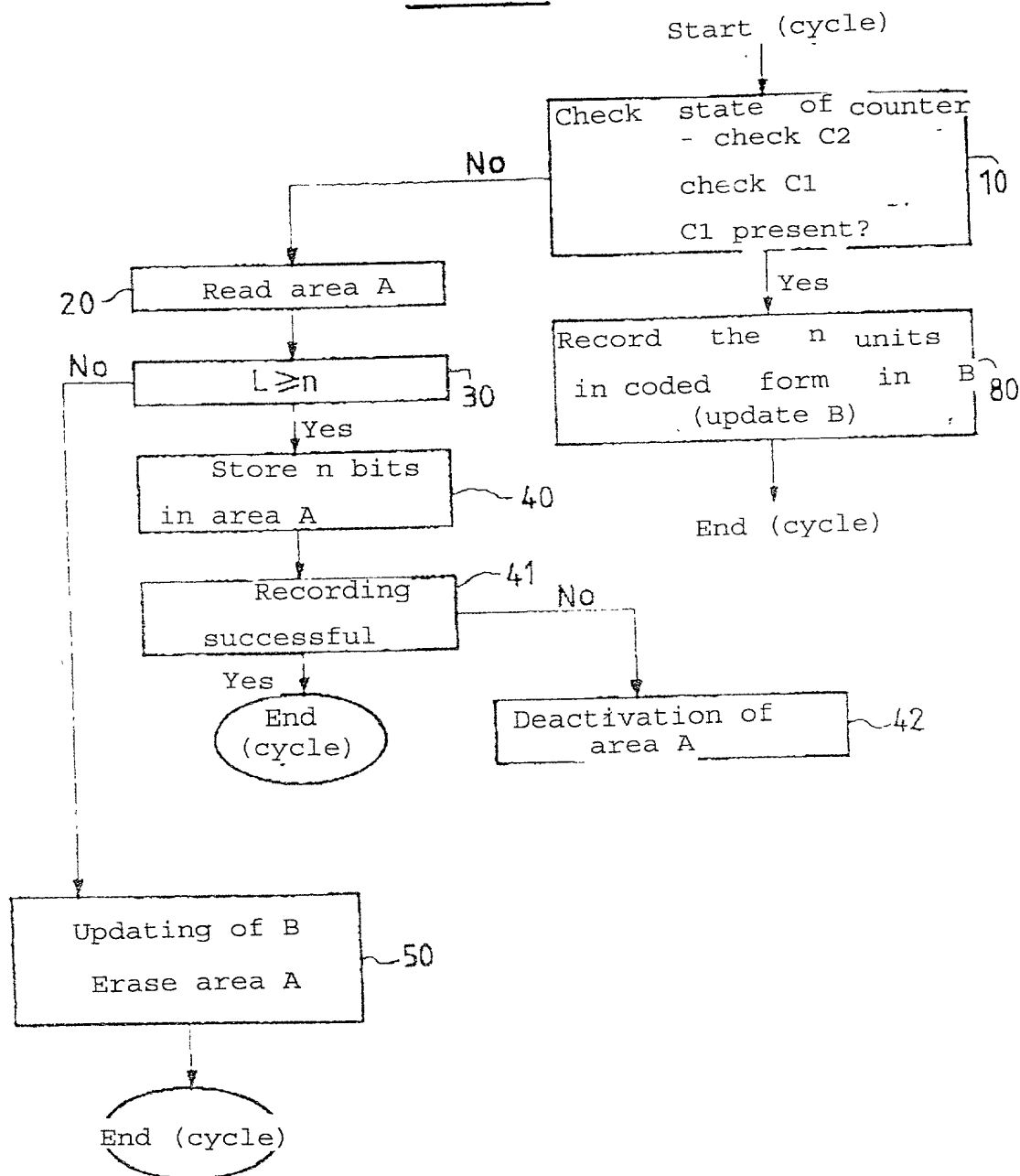
PCT/FR99/00292



WO 99/49646

PCT/FR99/00292

4/4

FIG_5

000250" 92594950

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (Includes Reference to Provisional and PCT International Applications)		Attorney's Docket No.																																
<p>As a below named inventor, I hereby declare that: My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:</p> <p><u>METHOD FOR SECURELY MANAGING A UNIT'S</u> <u>COUNTER AND SECURITY MODULE IMPLEMENTING SAID METHOD</u></p> <p>the specification of which (check only one item below):</p> <ul style="list-style-type: none">• is attached hereto.• was filed as a United States application Number _____ on _____ and was amended on _____ (if applicable).• was filed as a PCT international application Number <u>PCT / FR 99 / 00292</u> on <u>10/02/1999</u> and was amended on _____ (if applicable). <p>Thereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.</p> <p>I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.</p> <p>Thereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:</p> <table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th colspan="4" style="text-align: left; padding: 5px;">PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119:</th></tr><tr><th style="width: 25%; text-align: center; padding: 5px;">COUNTRY (if PCT, indicate "PCT")</th><th style="width: 25%; text-align: center; padding: 5px;">APPLICATION NUMBER</th><th style="width: 25%; text-align: center; padding: 5px;">DATE OF FILING (day, month, year)</th><th style="width: 25%; text-align: center; padding: 5px;">PRIORITY CLAIMED UNDER 35 U.S.C. § 119</th></tr></thead><tbody><tr><td style="text-align: center; padding: 5px;"><u>PCT</u></td><td style="text-align: center; padding: 5px;"><u>WO 99/49646</u></td><td style="text-align: center; padding: 5px;"><u>30/09/1999</u></td><td style="text-align: center; padding: 5px;"><u>Yes</u> <u>No</u></td></tr><tr><td style="text-align: center; padding: 5px;"><u>FRANCE</u></td><td style="text-align: center; padding: 5px;"><u>98 03483</u></td><td style="text-align: center; padding: 5px;"><u>20/03/1998</u></td><td style="text-align: center; padding: 5px;"><u>Yes</u> <u>No</u></td></tr><tr><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"><u>Yes</u> <u>No</u></td></tr><tr><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"><u>Yes</u> <u>No</u></td></tr><tr><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"></td><td style="text-align: center; padding: 5px;"><u>Yes</u> <u>No</u></td></tr></tbody></table> <p>Thereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.</p> <table style="width: 100%;"><tr><td style="width: 50%; text-align: center; padding: 10px;">_____ (Application Number)</td><td style="width: 50%; text-align: center; padding: 10px;">_____ (Filing Date)</td></tr><tr><td style="text-align: center; padding: 10px;">_____ (Application Number)</td><td style="text-align: center; padding: 10px;">_____ (Filing Date)</td></tr></table>			PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119:				COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119	<u>PCT</u>	<u>WO 99/49646</u>	<u>30/09/1999</u>	<u>Yes</u> <u>No</u>	<u>FRANCE</u>	<u>98 03483</u>	<u>20/03/1998</u>	<u>Yes</u> <u>No</u>				<u>Yes</u> <u>No</u>				<u>Yes</u> <u>No</u>				<u>Yes</u> <u>No</u>	_____ (Application Number)	_____ (Filing Date)	_____ (Application Number)	_____ (Filing Date)
PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119:																																		
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119																															
<u>PCT</u>	<u>WO 99/49646</u>	<u>30/09/1999</u>	<u>Yes</u> <u>No</u>																															
<u>FRANCE</u>	<u>98 03483</u>	<u>20/03/1998</u>	<u>Yes</u> <u>No</u>																															
			<u>Yes</u> <u>No</u>																															
			<u>Yes</u> <u>No</u>																															
			<u>Yes</u> <u>No</u>																															
_____ (Application Number)	_____ (Filing Date)																																	
_____ (Application Number)	_____ (Filing Date)																																	

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)
(Includes Reference to Provisional and PCT International Applications)

Attorney's Docket No.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)		
WO 99/49646	30/09/1999			

I hereby appoint the following attorney and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Michael J. Ure	33,089
Platon N. Mandros	22,124	James W. Peterson	26,057	Charles F. Wieland III	33,096
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Bruce T. Wieder	33,815
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Todd R. Walters	34,040
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Ronni S. Jillions	31,979
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunt	25,423	Harold R. Brown III	36,341
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Allen R. Baum	36,086
Regis E. Slutter	26,999	Bruce J. Boggs, Jr.	32,344	Steven M. duBois	35,023
Samuel C. Miller, III	27,360	William H. Benz	25,952	Brian P. O' Shaughnessy	32,747
Robert G. Mukai	28,531	Peter K. Skiff	31,917	Kenneth B. Leffler	36,075
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195	Fred W. Hathaway	32,236
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		



21839

and:

Address all correspondence to:



21839

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: James A. LaBarre

at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and PCT International Applications)	Attorney's Docket No.
--	-----------------------

FULL NAME OF SOLE OR FIRST INVENTOR XAVIER BANCHELIN		SIGNATURE <i>[Signature]</i>	DATE 29/08/00
RESIDENCE 123 CHEMIN DES AMARILLIS		CITIZENSHIP FRENCH	
POST OFFICE ADDRESS 13012 MARSEILLE - FRANCE JRX			
FULL NAME OF SECOND JOINT INVENTOR, IF ANY RIREILLE PAQUAC		SIGNATURE <i>[Signature]</i>	DATE 04/09/00
RESIDENCE Res. Clair Soleil, Bat B Traverse des Aude		CITIZENSHIP French	
POST OFFICE ADDRESS 13400 AUBAGNE - FRANCE JRX			
FULL NAME OF THIRD JOINT INVENTOR, IF ANY CAROLE-ANDREY KOCH-HODANIEZ		SIGNATURE <i>[Signature]</i>	DATE 06/09/2000
RESIDENCE Im. Le Garbrier, apt 600 280 bd Michelet 13008 Marseille		CITIZENSHIP FRENCH	
POST OFFICE ADDRESS			
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			